УДК 681.3.06

АЛГОРИТМИ ГЕНЕРАЦІЇ БАЗОВИХ ТОЧОК ЕЛІПТИЧНИХ КРИВИХ ЕДВАРДСА З ВИКОРИСТАННЯМ КРИТЕРІЇВ ПОДІЛЬНОСТІ ТОЧКИ

А. А. Вихло[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

У даній роботі наведено порівняльний аналіз нових та класичних алгоритмів генерації базової точки еліптичної кривої у формі Едвардса, виконано реалізацію цих алгоритмів, що допомогло підтвердити коректність їх роботи.

Ключові слова: еліптичні криві Едварса, базова точка

Вступ

Еліптичні криві в формі Едвардса над простим полем на теперішній час являються найбільш швидкими і перспективними для використання в асиметричних криптосистемах. Особливо важливі такі їх властивості [1], як рекордна швидкість, універсальність закону додавання, а також можливість представлення нейтрального елемента в афінних координатах.

У роботі [2] сформульовані і обґрунтовані критерії подільності точки кривої Едвардса на довільне натуральне число, з використанням яких розроблені алгоритми отримання кореня довільної степені із точки кривої, або в термінах адитивної групи алгоритми знаходження точки ділення на довільне натуральне число. У цій статті на основі цих критеріїв розроблені нові алгоритми обчислення координат базової точки кривої (або твірного елемента підгрупи простого порядку n групи точок кривої), а також виконано детальний порівняльний аналіз нових і класичного алгоритмів обчислення базової точки кривої; показано, що запропоновані далі алгоритми мають виграш в швидкодії в сотні разів. Цей виграш збільшується з ростом характеристики простого поля, над яким побудована крива.

Зауважимо, що приведені критерії подільності і алгоритми отримання кореня в групі точок еліптичної кривої є схожими на аналогічні критерії, отримані в [3] для простих полів і скінченних кілець. Але для еліптичних кривих ці алгоритми мають набагато більше прикладне значення.

1. Основні означення та позначення

Нехай крива Едвардса задана рівнянням

$$x^2 + y^2 = c^2(1 + dx^2y^2), \left(\frac{d}{p}\right) = -1 \qquad (1)$$

де $\left(\frac{d}{p}\right)$ – символ Якобі.

[a] antonvykhlo@gmail.com

Відповідно [1] всі криві, задані рівнянням (1) з параметрами c і d, в загальному виді ізоморфні кривим в формі

$$x^2 + y^2 = 1 + dx^2y^2, \left(\frac{d}{p}\right) = -1 \qquad (2)$$

Далі використовується саме форма (2). Позначимо E_p криву Едвардса над полем, $P = (x, y)$ або (x, y) – її довільна точка P, що має координати (x, y), де $x, y \in F_p$.

Як відомо, множина точок кривої створює групу відносно деякої специфічної операції, яку прийнято називати додаванням. Далі будемо використовувати так званий модифікований закон додавання, визначений наступним чином:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1x_2 - y_1y_2}{1 - dx_1x_2y_1y_2}, \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}\right) \qquad (3)$$

Нехай $P \in E_p, k \in N$, будемо говорити, що точка P ділиться на k, якщо $\exists R \in E_p : P = kR$, де під виразом kR розуміємо k-кратне додавання R (множення точки R на скаляр k, або скалярне множення)

Множину точок E_p , що діляться на k, ми будемо позначати $T_k(E_p)$.

Нехай $P \in T_k(E_p)$. Будемо говорити, що R являється коренем k-го степеню з P, якщо $kR = P$.

2. Постановка задачі

Основною задачею даної роботи є реалізація алгоритмів генерації базової точки кривої Едвардса, використовуючи криві, що зазначені в роботі [4], що дає змогу підтвердити коректність алгоритмів та правильність переліку знайдених базових точок[4]. Провести порівняльний аналіз нових і класичних алгоритмів, на основі якого зробити висновки відносно швидкодії.

2.1. Критерій подільності точки кривої Едвардса на 2

В роботі [5] сформульовано і доведено критерій подільності точки на 2.

Теорема 1 [5] (критерій подільності на два).

Нехай $P = (a, b) \in E_p$. Тоді наступні умови рівносильні:

1) $P \in T_2(p)$
2) $\frac{1-b^2}{p} = 1$

2.2. Критерій подільності точки кривої Едвардса на 4

Сформулюємо критерій подільності точки $P = (a, b)$ на 4

Теорема 2 (критерій подільності на чотири)

Нехай $P = (a, b) \in T_2(E_p)$. Позначимо s_1 довільник корінь із $1 - b^2$, а s_2 корінь із $1 - db^2$, такий що $(1 - s_1)(1 - s_2) \notin Q_p$

Тоді наступні умови рівносильні:

1) $P \in T_4(p)$
2) $(a + 1)s_2(1 - s_2) \notin Q_p$

3. Порівняльний аналіз алгоритмів генерації базової точки кривої Едвардса

Розглянемо три алгоритми генерації базової точки: класичний(використовується, наприклад, в алгоритмі ДСТУ 4145-2002), оснований на теоремі 1 і оснований на теоремі 2. Проведемо їх порівняльний аналіз швидкодії і деяким іншим факторам.

Алгоритм 2 (ДСТУ 4145-2002)

Вхід: еліптична крива $E(F_p)$.

1) Випадково вибираємо точку $P = (x, y) \in E(F_p)$.
2) Якщо $a \in \{0, 1, -1\}$, то перейти до п.1.
3) Обчислюємо nP.
4) Якщо $nP \neq O$, повертаємося до п.1.

Вихід: $P = (x, y)$ – базова точка.

Час роботи: Алгоритм використовує приблизно $log(p)$ операцій додавання точок. При кожному їх додаванні виконується шість множень ($6log^2(p)$ бітових операцій), шість операцій ділення із залишком ($2log^3(p)$ бітових операцій) і два алгоритми Евкліда ($2log^3(p)$ бітових операцій). Тому загальний час роботи алгоритму складає $96log^3(p)+4log^4(p)$ (з урахуванням того, що середнє число кількості кроків до успіху дорівнює чотирьом).

Наступний алгоритм 3 використовує теорему 1. В п.2 алгоритму перевіряється виконання умови теореми 1; якщо воно виконується, то згідно з теоремою отримана точка ділиться на 2 і для побудови базової точки її достатньо подвоїти. Якщо умова 1 не виконується, то точка, отримана перестановкою координат, буде ділитись на 2, а точка, отримана в результаті її подвоєння, буде ділитись на 4, тобто буде базовою точкою.

Алгоритм 3

Вхід: еліптична крива $E(F_p)$.

Вихід: $P = (x, y)$ – базова точка.

1) Випадково вибираємо точку $P = (x, y) \in E(F_p)$.
2) Якщо $a \in \{0, 1, -1\}$, то перейти до п.1.
3) Якщо $1 - b^2 \notin Q_p$, то $c \leftarrow a, a \leftarrow b, b \leftarrow c$.
4) Обчислюємо $P \leftarrow 2P$

Час роботи: Алгоритм використовує одне множення і одне ділення з залишком ($2log^2(p)$ бітових операцій), одну перевірку квадратичності ($2log^3(p)$ бітових операцій) і одне подвоєння точки ($12log^2(p)+2log^3(p)$ бітових операцій). Всього $14log^2(p)+4log^3(p)$ бітових операцій.

Наступний алгоритм побудований аналогічно алгоритму 3, але використовує теорему 2. Він фактично є алгоритмом перевірки подільності на 4. Дійсно, будь-яка точка $P \in T_4(E_p)$, така, що $P \neq O$, де $O = (1, 0)$, являється базовою точкою.

Алгоритм 4

Вхід: еліптична крива $E(F_p)$.

Вихід: $P = (x, y)$ – базова точка.

1) Випадково вибираємо точку $P = (x, y) \in E(F_p)$.
2) Якщо $a \in \{0, 1, -1\}$, то перейти до п.1.
3) Якщо $1 - b^2 \notin Q_p$, то $c \leftarrow a, a \leftarrow b, b \leftarrow c$.
4) Обчислити $s_1 = \sqrt{1 - b^2}, s_2 = \sqrt{1 - db^2}$ (будь-який з двох можливих коренів).
5) Якщо $(1 - s_1)(1 - s_2) \in Q_p$, то $s_2 \leftarrow p - s_2$.
6) Якщо $(a + 1)s_2(1 - s_2) \in Q_p$, то перейти до п.1.

Час роботи: Алгоритм використовує два множення і два ділення з остатком ($4log^2(p)$ бітових операцій), одне обчислення кореня ($2log^3(p)$ бітових операцій) і дві перевірки квадратичності ($4log^3(p)$ бітових операцій). Зауважимо, що алгоритм 4 є ймовірнісним; при цьому середня кількість кроків до успіху дорівнює двом. Тому час роботи алгоритму складає $12log^3(p) + 8log^2(p)$ бітових операцій.

Висновки

Практичними результатами являються, в першу чергу, реалізація нових алгоритмів генерації базової точки кривої Едвардса. Також приведено порівняльний аналіз нових і класичних алгоритмів генерації базової точки. Перевірено коректність базових точок для еліптичних кривих, зазначених в роботі [4].

За результатами дослідження можна зазначити, що наведені нові алгоритми генерації базової точки мають значний приріст в швидкодії. Використання еліптичних кривих в формі Едвардса значно підвищить швидкодію алгоритмів цифрового підпису завдяки властивостям, зазначених в даній роботі .

Перелік використаних джерел

1. D.J. Bernstein. . Faster addition and doubling on elliptic curves. — 3 edition. — 2007. — P. 29–50 c.
2. Ковальчук Л.В Бессалов А.В Беспалов О.Ю. Алгоритмы генерации базовой точки с использованием критериев делимости точки кривой. — 2013.
3. Л.В. Ковальчук. . Рекурентні алгоритми обчислення кореню довільного степеню у кільці лишків. — 2013. — С. 58–66 с.
4. А.А. Бессалов А.В. Дихтенко. Криптостойкие кривые Эдвардса над простыми полями. — 2013.
5. А.В. Бессалов. Новые свойства кривой Эдвардса над простым полем. — 2015. — С. 137–143 с.